iPhone Configuration Creation and Deployment

Session 602

These are confidential sessions—please refrain from streaming, blogging, or taking pictures.

iPhone Configuration Creation and Deployment

Are you in the right room?

Stan Jirman
iPhone Applications Nerd

What You'll Learn

- What configuration profiles are and when to use them
- What you can configure using a profile
- An overview of the profile file format
- How to create a profile
- How to deploy a profile

What Are Configuration Profiles?

Configuration Profiles

- Small XML files that hold settings for iPhone and iPod touch
- Configure common yet potentially complex settings such as networking or VPN
- Enforce a specified degree of security on the iPhone
- Install or enroll credentials on the iPhone
- Do all of this securely
- Not to be confused with provisioning profiles, which allow an iPhone to run applications—This session is not about provisioning profiles

Configuration Profiles Define…

Microsoft Exchange ActiveSync (EAS) account settings

Passcode policies and restrictions

Credentials (certificates)

VPN configuration information

Wi-Fi settings

Application access restrictions

Mail settings

APN settings

Web clips

SCEP settings

LDAP

CalDav

CalSub

Configuration Profiles Define…

- Microsoft Exchange ActiveSync (EAS) account settings
- Passcode policies and restrictions
- Credentials (certificates)
- VPN configuration information
- Wi-Fi settings
- Application access restrictions
- Mail settings
- APN settings
- Web clips
- SCEP settings
- LDAP
- CalDav
- CalSub

Microsoft Exchange Settings

- Sets up an EAS account
  - Email
  - Calendar
  - Address book
- EAS can enforce a level of security
  - Passcode strength
  - iPhone lock
  - Remote wipe
  - Camera off
  - More policies
- Certificate Based Authentication

Configuration Profiles Define…

- Microsoft Exchange ActiveSync (EAS) account settings
- Passcode policies and restrictions
- Credentials (certificates)
- VPN configuration information
- Wi-Fi settings
- Application access restrictions
- Mail settings
- APN settings
- Web clips
- SCEP settings
- LDAP
- CalDav
- CalSub

Passcode Policies

- Define passcode requirements for the iPhone
  - Minimum passcode length and “quality”
  - Passcode expiration
- Applied in conjunction with your EAS policies
- Policies are merged
  - Multiple profiles could specify different policies
  - EAS could define different policies than a profile

Passcode Policy Merging

- Most stringent of each policy taken
  - Policy A:
    - Six characters
    - Passcode expires in 30 days
  - Policy B:
    - Four characters
    - Minimum two special characters
  - Merged “synthesized” policy:
    - Six characters
    - Minimum two special characters
    - Passcode expires in 30 days

Configuration Profiles Define…

Microsoft Exchange ActiveSync (EAS) account settings

Passcode policies and restrictions

Credentials (certificates)

VPN configuration information

Wi-Fi settings

Application access restrictions

Mail settings

APN settings

Web clips

SCEP settings

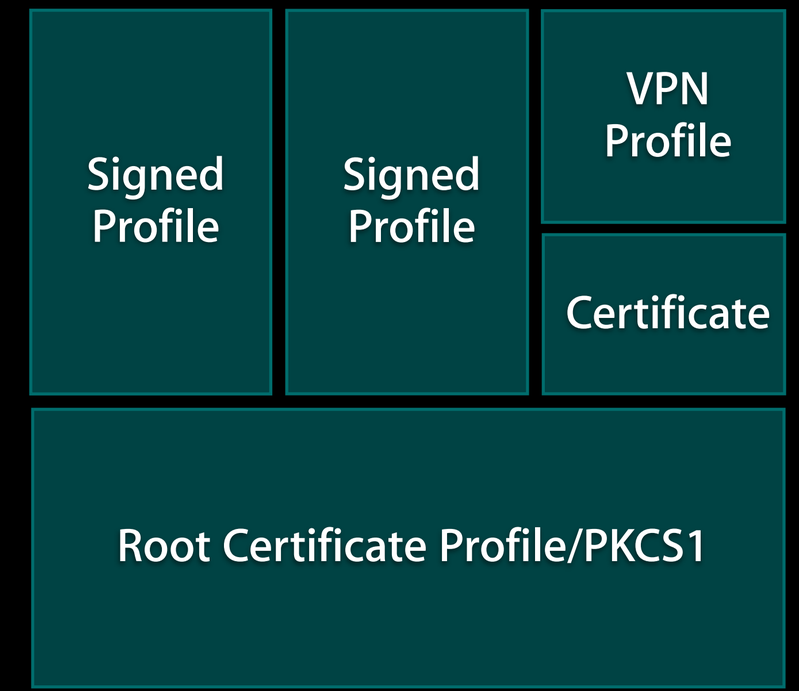
LDAP

CalDav

CalSub

Credentials/Certificates

- Either embedded in a profile, or raw PKCS#1 or PKCS#12 file
- Organizations can install own signing certificates
- All actual configuration profiles then can be signed with this certificate
- Authentication Identities
  - VPN
  - Wi-Fi
  - EAS Improved
- Details to be discussed soon



Configuration Profiles Define…

Microsoft Exchange ActiveSync (EAS) account settings

Passcode policies and restrictions

Credentials (certificates)

VPN configuration information

Wi-Fi settings

Application access restrictions

Mail settings

APN settings

Web clips

SCEP settings

LDAP

CalDav

CalSub

VPN Configuration

- Protocols
  - PPTP
  - L2TP
  - IPSec (Cisco)
- Authentication X.509 Identity
  - IPSec
- Proxies

Configuration Profiles Define…

Microsoft Exchange ActiveSync (EAS) account settings

Passcode policies and restrictions

Credentials (certificates)

VPN configuration information

Wi-Fi settings

Application access restrictions

Mail settings

APN settings

Web clips

SCEP settings

LDAP

CalDav

CalSub

Wi-Fi Settings

- Visible and hidden networks
- Preshared key and 802.1x encryption
  - WEP
  - WPA
  - WPA2
- 802.1x
  - Authentication protocols
    - TLS, LEAP, TTLS, PEAP, EAP-FAST, and MS-CHAPv2
  - Credentials
    - X.509 identities
    - One-time passwords

Configuration Profiles Define…

Microsoft Exchange ActiveSync (EAS) account settings

Passcode policies and restrictions

Credentials (certificates)

VPN configuration information

Wi-Fi settings

Improved

Application access restrictions

Mail settings

APN settings

Web clips

SCEP settings

LDAP

CalDav

CalSub

New

Application Access Restrictions

- Disallow the use of specific applications
  - YouTube
  - Safari
  - iTunes Music Store
  - iTunes Application Store/application installation through iTunes
  - Camera Improved
- Disallow access to explicit media content in iPod application

Configuration Profiles Define…

- Microsoft Exchange ActiveSync (EAS) account settings
- Passcode policies and restrictions
- Credentials (certificates)
- VPN configuration information
- Wi-Fi settings
- Application access restrictions
- Mail settings
- APN settings
- Web clips
- SCEP settings
- LDAP
- CalDav
- CalSub

Mail Accounts

- Create a complete configuration, or a template
  - Protocol
  - Host
  - Account name
  - Account password

  - Authentication scheme
  - SSL
- Create a template of any subset of the above; iPhone UI will ask for missing pieces when the profile is installed

Configuration Profiles Define…

Microsoft Exchange ActiveSync (EAS) account settings

Passcode policies and restrictions

Credentials (certificates)

VPN configuration information

Wi-Fi settings

Application access restrictions

Mail settings

APN settings

Web clips

SCEP settings

LDAP

CalDav

CalSub

APN Settings

- Analogous to a Wi-Fi base station, just for cellular network
- Typically used by large corporations
- Access to APN controlled via username/password
- Specify HTTP proxy

Configuration Profiles Define…

Microsoft Exchange ActiveSync (EAS) account settings

Passcode policies and restrictions

Credentials (certificates)

VPN configuration information

Wi-Fi settings

Application access restrictions

Mail settings

APN settings

Web clips

SCEP settings

LDAP

CalDav

CalSub

Web Clips

- Predefined web clips on Springboard “desktop”
- Optionally nonremovable
- Allow e.g. quick access to corporate web pages

Configuration Profiles Define…

Microsoft Exchange ActiveSync (EAS) account settings

Passcode policies and restrictions

Credentials (certificates)

VPN configuration information

Wi-Fi settings

Application access restrictions

Mail settings

APN settings

Web clips

SCEP settings

LDAP

CalDav

CalSub

SCEP Settings

- SCEP service:
  - Base URL of service
  - Name of instance
- Input to Certificate Signing Request (CSR):
  - Key type and size
  - Challenge to preauthenticate the enrollment request
  - Subject

Configuration Profiles Define…

Microsoft Exchange ActiveSync (EAS) account settings

Passcode policies and restrictions

Credentials (certificates)

VPN configuration information

Wi-Fi settings

Application access restrictions

Mail settings

APN settings

Web clips

SCEP settings

LDAP

CalDav

CalSub

LDAP

- Directory service
- Each LDAP account supports multiple search settings (search parameters within an account)
- Search settings are exposed in the Groups UI in Address Book and Phone
- All search settings are queried to provide autocomplete when composing emails

Configuration Profiles Define…

- Microsoft Exchange ActiveSync (EAS) account settings
- Passcode policies and restrictions
- Credentials (certificates)
- VPN configuration information
- Wi-Fi settings
- Application access restrictions
- Mail settings
- APN settings
- Web clips
- SCEP settings
- LDAP
- CalDav
- CalSub

CalDAV

- OS X Server's Calendaring solution
- Synchronizes calendars wirelessly
- It is fun

Configuration Profiles Define…

Microsoft Exchange ActiveSync (EAS) account settings

Passcode policies and restrictions

Credentials (certificates)

VPN configuration information

Wi-Fi settings

Application access restrictions

Mail settings

APN settings

Web clips

SCEP settings

LDAP

CalDav

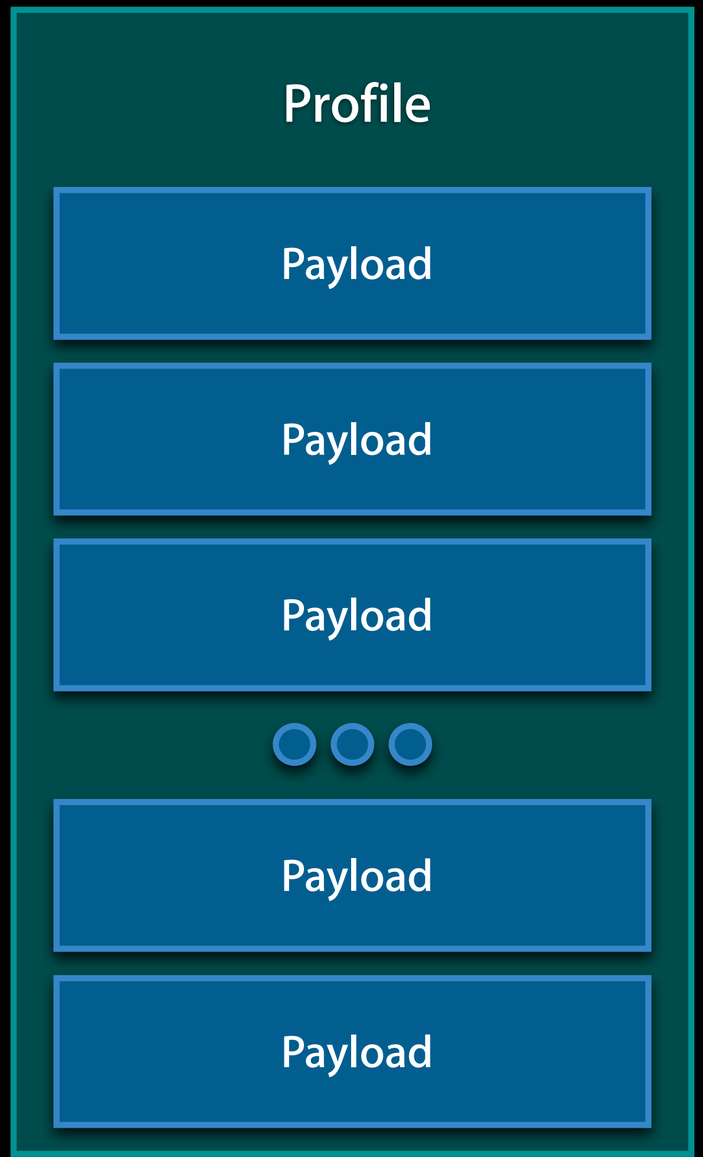
CalSub

Calendar Subscriptions

- List of calendars on Apple website you can subscribe to
- You can publish subscribed calendars through iCal; other people can subscribe on iPhone
- Subscribed calendars published on Google
- You can optionally authenticate with a username/password

Flexible Profile Contents

- A profile can configure:
  - Any single component
  - Virtually any combination of components
- Convenience
- “Carrot and Stick” approach
  - I give you access to my network and servers…
  - …but you will play by my rules



Carrot and Stick

- Carrot
  - Provide users with a certificate-based VPN
  - Give them access to your 802.1x Wi-Fi network
- Stick: Make them abide by your rules
  - Enforce passcode quality and renewal
  - Enforce iPhone locking
  - Disallow music and application store
  - Disallow installation of third-party apps

Content Restrictions

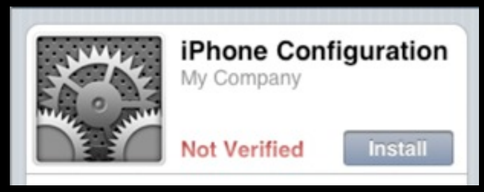
- Each profile can contain only one of the following:
  - Passcode policy
  - Application access
  - Removal password
  - EAS
    - Only one EAS account overall, not just per profile

All or Nothing

- All profiles are all or nothing
  - All settings are accepted or none are applied
  - Prevents user from “cherry-picking” the settings
    - For example, the ability to connect to a VPN comes at the price of a mandatory passcode
- Profile removal is also all or nothing
  - Can be regulated
    - Password protected
    - Completely prevented
      - Evil, unethical, possibly flat out illegal

Signing the Profiles

- You should sign all profiles (iPCU makes it easy!!)
- Profiles are either Verified, Not Verified, or Unsigned
- The root certificates necessary to verify a profile must be installed on the device for a profile to show as Verified
- Preinstalled root certificates on iPhone and iPod touch are the same as on Mac OS X
  - Keychain Access > System Roots to view them (600+)



Security?

- Profiles can be encrypted

- Sign them to avoid and detect tampering
  - A signed but modified profile will be always rejected
  - All encrypted profiles are always signed

- You can can now include sensitive information because profile is encrypted

  - iPhone will prompt for data you omit, such as passwords

Caveats

- No dependency analysis when removing a profile
  - Removal of one profile may render another one inoperable
- No conflict resolution
  - Installing a profile that even partially overlaps with an already installed profile will fail
  - Passcode policies are correctly merged across profiles
- No expiration date
  - Profiles and their contents live “forever” (until removed)

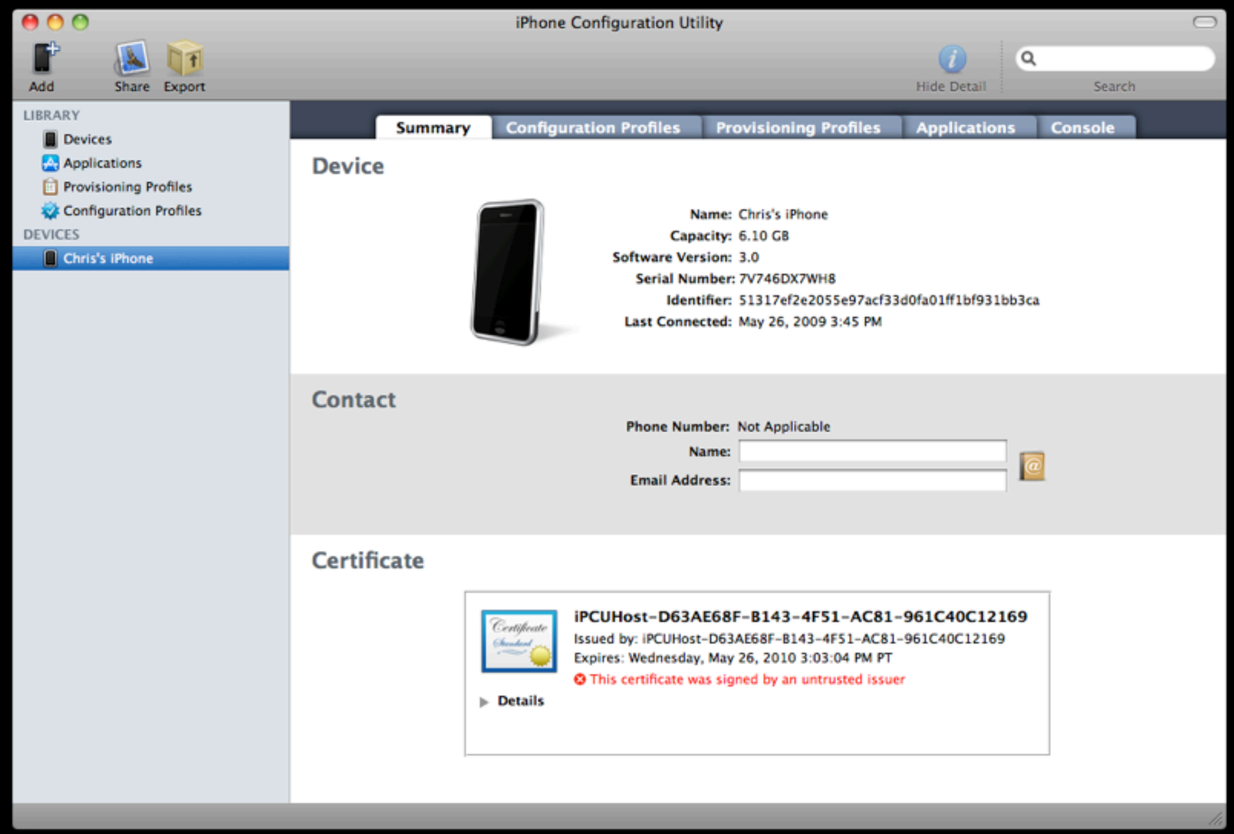
Profile File Format

- Straightforward XML
- Same DTD as all other Mac OS X XML plists
- Simple content format with lots of shared properties
- Profile XML spec is available

Creating Profiles

Creating Profiles

- iPhone Configuration Utility
  - For Mac OS X
  - For Windows



iPhone Configuration Utility

- iPhone Configuration Utility
  - Serves as curator for configuration and provisioning profiles
  - Creates configuration profiles
  - Encrypts and signs configuration profiles
  - Displays console logs for attached iPhones

Demo

iPhone Configuration Utility

Chris Skogen
Developer Tools Engineer

Profile Deployment

Several Ways of Deploying

- Via email
- Via web
- Via USB tether from iPCU
- Over the air via profile distribution service

- USB and OTA always encrypted and device specific
- Email and Web delivery optionally encrypted and device specific
  - Suitable for generic, “open” and easy to get content

Profile Deployment

- Distributing via the web
  - "Pull" distribution—to a large/unknown pool of people
  - Profiles can be encrypted, but are then device specific and thus need to be generated on the fly
  - May be unencrypted for convenient delivery of nonsensitive settings
  - Use a password-protected website for download access
  - Distribute the URL via SMS

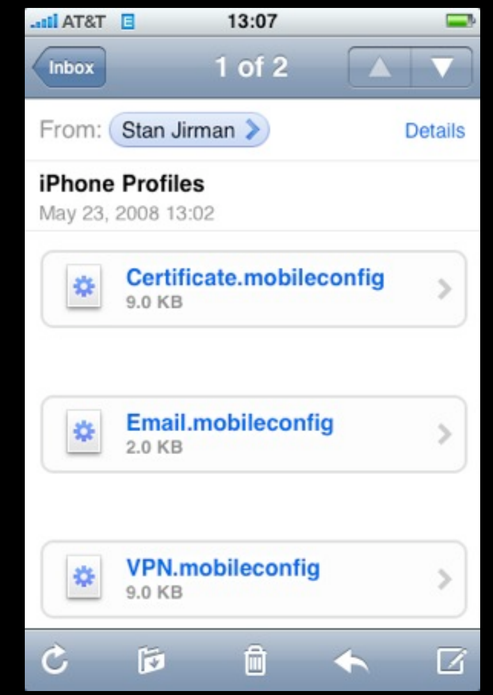
Distributing Profiles via Web

- Configure web server for the profiles MIME type

```
application/x-apple-aspen-config
mobileconfig
```

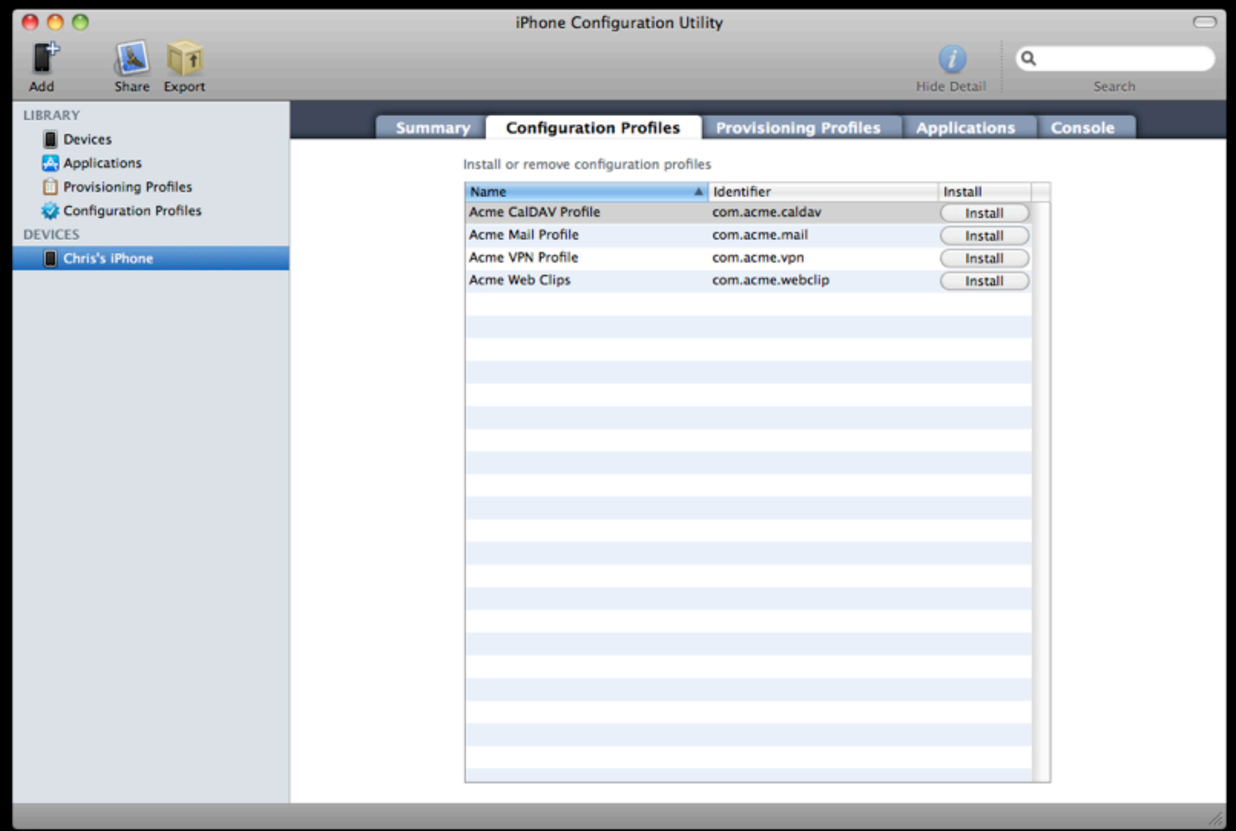
Profile Deployment

- Distributing via email
  - "Active" distribution—users don't need to remember/type a URL
  - Profile can be encrypted
  - Attach .mobileconfig file to an email, send to user
  - User doesn't have to be online to reinstall a profile
  - Not "real" push: No automatic updates of profiles
  - An email account has to be manually set up first
  - User still has to tap to install it



Profile Deployment

- Distributing via iPCU USB
  - "Active" distribution—direct connection required
  - Profile always encrypted
  - Creates device record for later reissue of profile
  - User or administrator still has to tap to install it



Profile Deployment

- OTA Distribution
- Fully encrypted
- Requires some form of authentication
- User still has to tap to install it

Profile Encryption and Distribution Service

If you really have to know

Conrad Sauerwald
Security Goon

Encrypted Profiles

- Signed using CMS Signed Data
- Policies, services and credentials are encrypted together
- Encrypted using CMS Enveloped Data
- Targeting specific device

Profile Distribution Service

- User and device authentication
  - Identify user
  - Device is iPhone
- Profile service certificate enrollment
- Generate user and device specific profile
- Profile update

Certificate Enrollment

- X.509 identities
  - Enrollment to avoid private key leaving device
- SCEP request preauthenticated (automatic mode)
- Enrollment used for
  - Profile service
  - Additional credentials (Certificate-based VPN authentication)

SCEP

- Practical choice for automatic enrollment
- RSA
- 1024 and 2048 bit keys
- Challenge for preauthentication
- iPhone client implementation still has interoperability issues

USB vs. OTA

- At a high level they function the same
- USB tether functions as trusted connection
- Updates need to be pushed with iPCU (email, web)
- OTA more involved upfront, but scales to more devices

Profile Distribution Service

Overview

0 Bootstrap URL

1 Authenticate Device and Get Enrollment Authorization

2 Enroll Certificate for Profile Service

Profile Service

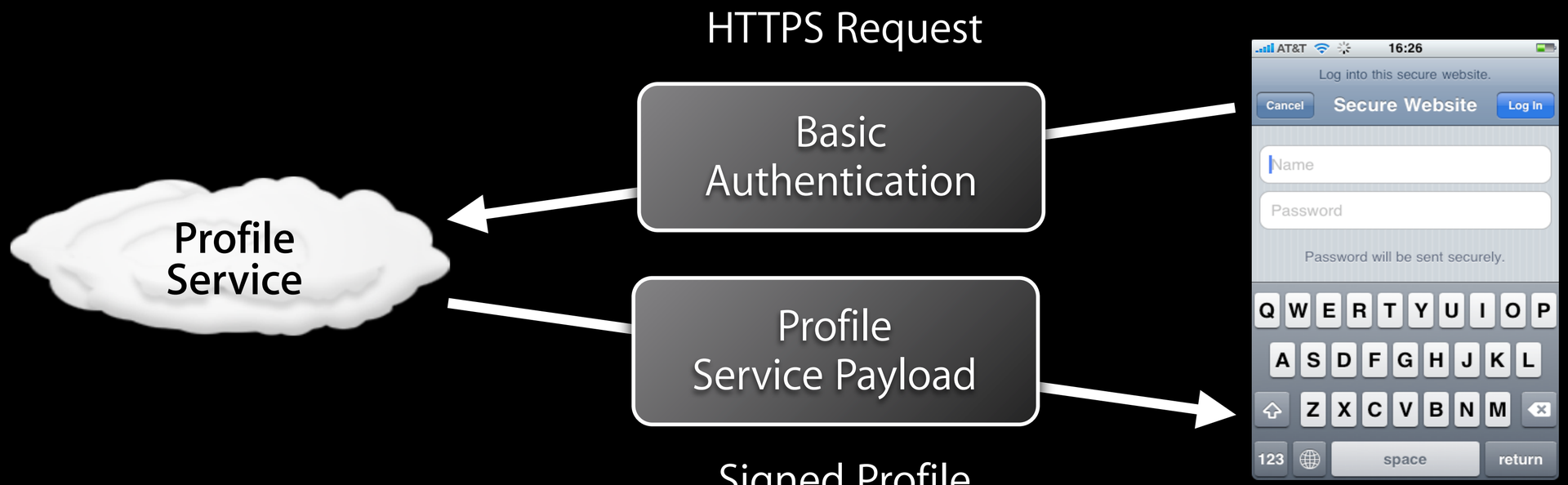
Certificate Authority

3 Get Encrypted Profile

4 Install Profile and Enroll Further Certificates

Profile Distribution Service

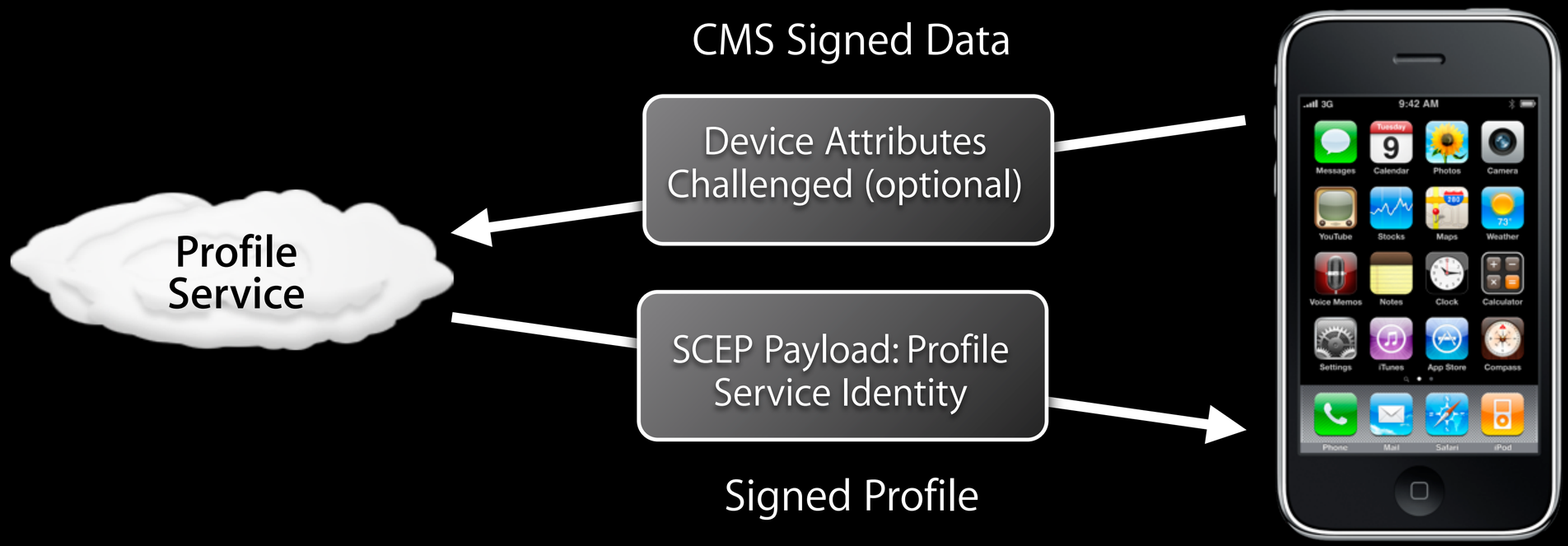
0. Bootstrap



- Optional authentication to identify the user
- Bootstrap profile contains URL, requested device attributes and optional authorization token to carry user authentication forward

Profile Distribution Service

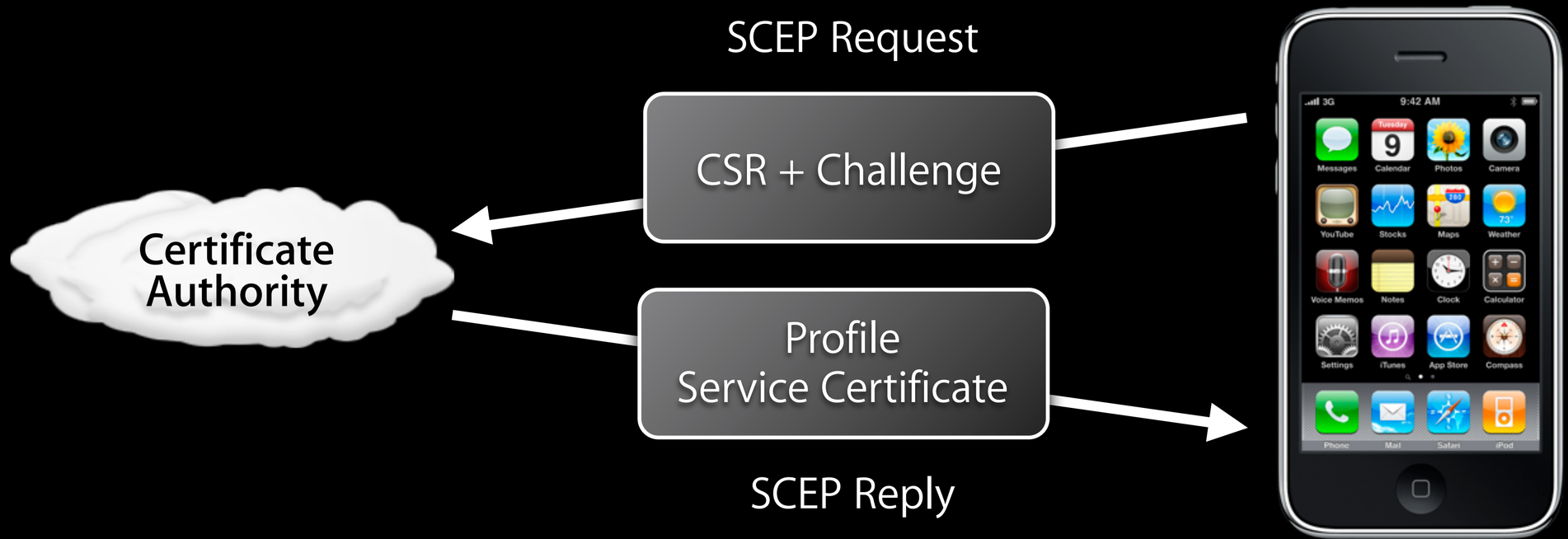
1. Authenticate Device



- Device provides Build, UDID, Type details, signed by device certificate
- Service provides SCEP details to enroll Profile Service identity

Profile Distribution Service

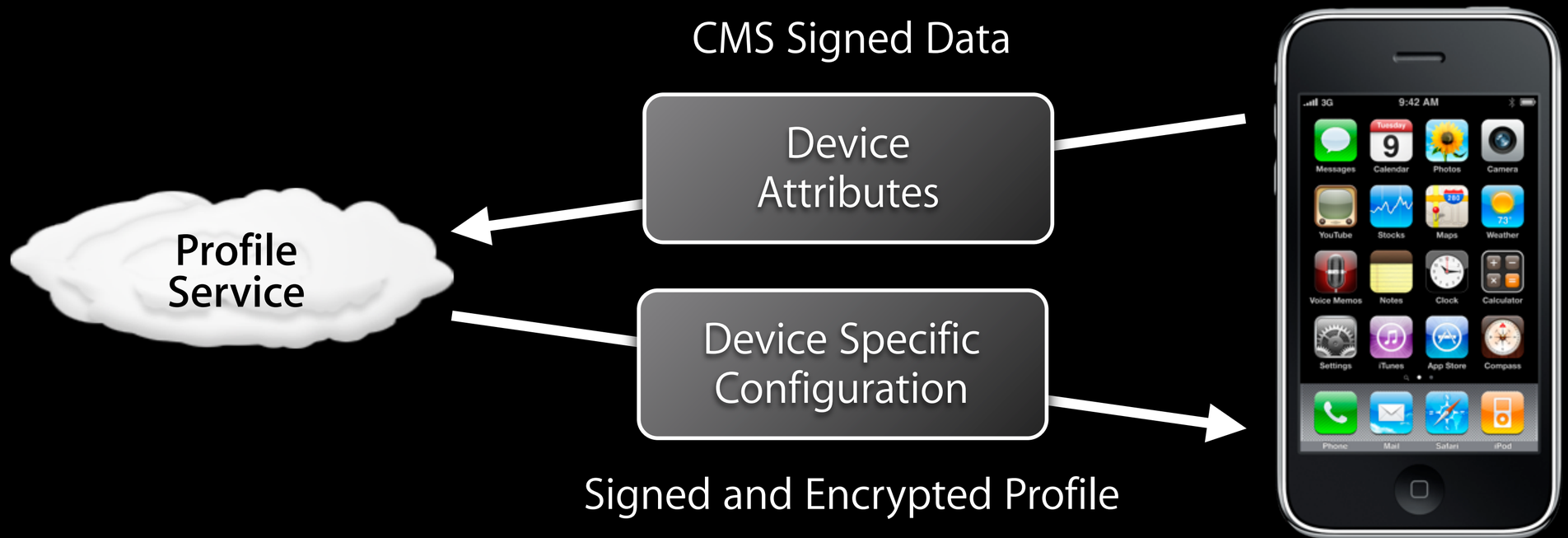
2. Enroll Certificate



- Device generates key
- Sends Certificate Signing Request (CSR) using SCEP
- Verifies reply and stores certificate

Profile Distribution Service

3. Get Profile



- Device authentication with profile service identity
- Device specific signed and encrypted profile returned
- Also used for profile updates

Profile Distribution Service

4. Install Profile

- Profile installs policies alongside services, which require credentials
- Credentials can be included or generated and enrolled

Profile Distribution Service

OTA Demo

Conrad Sauerwald
Core OS Engineer/Data Security

Profile Backup and Migration

- Profiles are backed up
  - Same iPhone will be configured identically after a restore via iTunes
  - If an encrypted profile is present, backup will be always encrypted (otherwise, backup encryption is optional)

- No migration
  - Restoring a new iPhone from a backup of a different iPhone will not restore profile settings
  - Certificates, passwords, and so on are not restored, they need to be reentered or reapplied via profile
  - Security feature for open cubicle landscape

Updating Profiles

- Utilize profile identifier to ensure updated profiles are replaced when installed on the iPhone
  - `com.MyCompany.chicagofield`
  - `com.MyCompany.santaclarafield`
- Profiles are not pushed to users; they must update them manually
- A signed profile can be updated only by another profile from the same signing authority

Removing Profiles

- Normally unrestricted
- Profiles may be flagged as nonremovable
  - Erase the iPhone
  - Enter optionally specified removal password (stored in the encrypted section of the profile)
  - Install an update of the same profile without the “do not remove” flag
    - Update profile must come from the same signing authority to avoid spoofing
  - Don’t go overboard with this flag
    - You will make the users’ lives really miserable
    - Legally questionable if your company doesn’t own the iPhone

Profile User Experience

Demo

Chris Pavicich
Developer Tools Engineer

Profile Deployment Best Practices

- Use OTA distribution for flexibility and scale
- Use USB/iPCU distribution for small shops
- Use unencrypted profiles on a web server for simple distribution of complex yet benign “public” settings
- Always sign profiles
  - iPhone will refuse to install a profile that has been tampered with

Summary

- Profiles simplify iPhone and iPod touch configuration
- iPCU available for Configuration Profile creation and deployment
- Encryption available to prevent tampering and snooping
- Distribute profiles via web, email or OTA servers
- Consider security when creating profile templates and choosing deployment method

Related Sessions

Integrating iPhone into the Enterprise	Mission Tuesday 9:00AM
iPhone Configuration Creation and Deployment	Information Technologies Lab Thursday 5:00 PM

More Information

Mark Malone
Technology Evangelist
mmalone@apple.com

Documentation
Enterprise Deployment Guide
http://www.apple.com/iphone

Apple Training and Certification
http://training.apple.com

Q&A

WWDC Session Survey

You can rate your sessions on the WWDC Attendee Site.

Survey forms are located on each session description page at:

developer.apple.com/wwdc/attendee

WWDC09